Crypto Chasers Confidential

Saturday, February 3, 2018
Follow our Telegram Channel for more high quality in depth analysis'
Follow us on Twitter

Zilliqa (ZIL) Analysis

Type: Token
Circulating Supply: 6,508,988,220 ZIL
Total Supply: 12,600,000,000 ZIL
Marketcap: $498,145,886 USD
Whitepaper Style: Highly technical

Official Website
Coinmarketcap
Source Code
Whitepaper

Coin Supply Statistics
According to a post from HackerNoon:

*At the Token Generation Event (TGE), Zilliqa set the cap for contributors to 48,889 ETH, or US$ 22 million at a locked rate of US$ 450/ETH. Zilliqa's tokens are called 'Zillings', or ZILs. ZIL price at the TGE was **US$ 0.003877**. Zilliqa has a finite supply of 21 billion tokens, of which only 60% (12.6 billion tokens) are generated at the TGE, and the remaining 40% (8.4 billion tokens) would be mining rewards over the next 10 years. The details on Zilliqa's TGE can be found of Zilliqa's official blog post regarding TGE.*

Zilliqa ICO statistics from ICODrop

📊 MARKET & RETURNS

ZIL token price
$0.0762995 (+8.58%)
0.0000797013 ETH
0.00000839 BTC

Returns since ICO

| 20.03x USD | 9.41x ETH | 33.63x BTC |

These numbers show how much the token price has changed relative to the initial ICO token price.

24h Volume	Market Cap
$12,216,000	**$496,632,547**

As you can see those who bought during the ICO have a high upside.

About

Taken from their official website:
Zilliqa is the world's first high-throughput public blockchain platform - designed to scale to thousands of transactions per second.

Zilliqa brings the theory of sharding to practice with its novel protocol that increases transaction rates as its network expands. The platform is tailored towards enabling secure data-driven decentralised apps, designed to meet the scaling requirements of machine learning and financial algorithms.
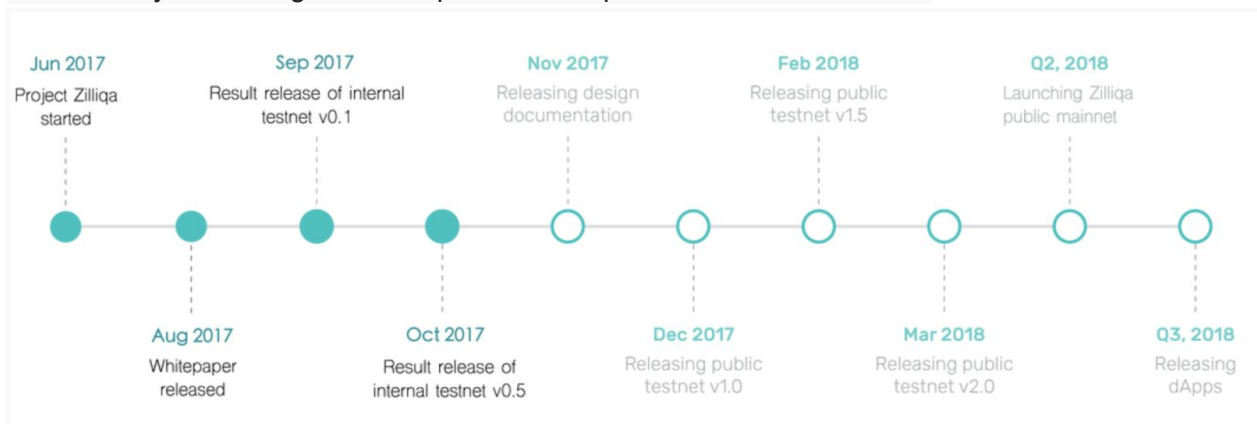
Zilliqa has been under research and development for two years, and powered several ground-breaking deployments commercially.

There is a lot of solid information available in the general FAQ section on their website, and also information in their whitepaper which we will later analyze that includes how they plan on reaching a high level of scalability, we encourage readers to take a look at the FAQ section as they get pretty technical in there as well, here's an excerpt:

In regards to their consensus mechanism:
The protocol has novel advances over what has been published by Zilliqa team members in scientific conference papers. It comprises of the overarching layer of directory committee, and a refinement of the PBFT protocol in each shard. Zilliqa employs Elliptic Curve Based Schnorr Signature Algorithm (EC-Schnorr) with multi-signing or signature aggregation. This means that the size of the signature stays small even when a lot of miners sign a block. Moreover, by leveraging efficient network topology, Zilliqa's consensus scheme reduces the communication complexity to O(N), i.e., linear to the size of the network.

It's also very refreshing to see a quick roadmap on their official website:

Jun 2017	Sep 2017	Nov 2017	Feb 2018	Q2, 2018
Project Zilliqa started	Result release of internal testnet v0.1	Releasing design documentation	Releasing public testnet v1.5	Launching Zilliqa public mainnet

Aug 2017	Oct 2017	Dec 2017	Mar 2018	Q3, 2018
Whitepaper released	Result release of internal testnet v0.5	Releasing public testnet v1.0	Releasing public testnet v2.0	Releasing dApps

Looks like Zilliqa is following the model of Nebulas or EOS and many other coins in which they have a token and release their mainnet later this year.

Let's take a look at the team, in this case as this is a quite multi-faceted almost Ethereum-like blockchain project that can be applicable to any industry - we expect the team to be highly sophisticated. We expect the CEO to be a superstar having worked on blockchain or finance projects before and have years of experience in finance or technology. We expect the development team to be very active developing the project on GitHub and have much experience in open source software development. The technical requirements for this project to be a success are very high - the team must be adept at cryptography concepts as well as implementing them from scratch.

Team

Xinshu Dong

Title: CEO of Zilliqa
LinkedIn, **Twitter**, **Personal Website**

Xinshu's LinkedIn bio:
Computer security expert currently developing secure and scalable blockchain.

Used to work on several other aspects of systems security as well, including defenses against the threats to web applications, web browsers, mobile platforms, and cyber-physical systems (e.g., smart grid, transportation systems).

Presently keen to applying the technologies he developed to revolutionising the resilience and scalability of software systems.

The first thing that is a huge positive for us is the fact that this guy has a PhD from a legitimate university in Computer Science - kind of rare in the space (which is sad) to see someone have that high level of an education.

Education

National University of Singapore
Doctor of Philosophy (PhD), Computer Science
2008 – 2013

East China Normal University
B.E., Software Engieering
2004 – 2008

Let's take a look at his previous experience

Experience

CEO
Zilliqa
Aug 2017 – Present • 7 mos

Zilliqa: the scalable blockchain for high throughput consensus computing
https://www.zilliqa.com

Head of Engineering
Anquan Capital
Jul 2017 – Present • 8 mos

Senior Research Fellow
National University of Singapore
Jul 2016 – Jul 2017 • 1 yr 1 mo

Reseacher
Advanced Digital Sciences Center (ADSC), Illinois at Singapore Pte Ltd
Mar 2014 – May 2017 • 3 yrs 3 mos

Research Fellow
National University of Singapore
Jul 2013 – Mar 2014 • 9 mos

His second listed thing is "Head of Engineering" at Anquan Capital. What is Anquan Capital? Let's find out...
We found Anquan's personal website and they seem to be a research focused group working on a private and public blockchain as well as a hardware rooted trust technology - they even have

their own whitepaper - as this is an analysis dedicated to ZIL we won't analyze their whitepaper but we encourage readers to check them out.

We are impressed with Dr. Dong's prior experience and endeavors.

Pratik Saxena

Title: Chief Scientific Advisor

Dr. Saxena is also an assistant professor at the National University of Singapore and has had keynote talks regarding blockchain at large venues one of which you can view here. The thing that pops out the most as was the case with Dr. Dong is Dr. Saxena's vast educational experience:

Education

University of California, Berkeley
Doctor of Philosophy (Ph.D.), Computer Science
2008 – 2012

Stony Brook University
Master's Degree, Computer Science
2005 – 2007

University of Pune
Bachelor's Degree, Computer Engineering
2000 – 2004

Dr. Saxena is also part of the Anquan team. An article from BusinessWire dated November 12, 2017 talks about Dr. Saxena quite positively it lists:
The original scientific research for the project was done in the laboratory of Dr. Prateek Saxena, who is now Chief Scientific Officer with Zilliqa. Earlier projects and ventures that emerged from Dr. Saxena's research group include KyberNetwork, TrueBit, SmartPool, and Anquan Capital.

As of this writing Kyber Network is ranked 47th by marketcap on Coinmarketcap and Zilliqa is ranked 50th.

Core Developers
Siddharta Dutta - Based on LinkedIn looks like a strong developer with an education from India's prestigious Indian Institute of Technology, and prior software engineering experience at Microsoft.
Antonia Nunez - Worked at Anquan Capital as well as a developer has much experience coding C++ and other languages just from a quick skim of his Linkedin.

Based on what we have seen so far we rate the team as strong, you can go through the team yourself and do a more thorough analysis.

Whitepaper

As expected of a whitepaper coming out of a successful university lab it is highly technical - it provides reasons for the technology as well as the mathematical fundamentals behind the technology. For example, the whitepaper goes into detail of consensus mechanisms as well as the use of Schnorr Signatures in the Zilliqa blockchain. Read the entire whitepaper here.

GitHub

From the readme on their GitHub:

The current release has the following features implemented:

- *Proof of Work 1 (PoW1) and 2 (PoW2) for joining the network*
- *Network sharding*
- *Directory Service*
- *Consensus for DS block, Sharding structure, Shard Microblock and Final block*
- *EC-Schnorr signature*
- *Data layer and accounts store*
- *Looking up nodes to allow new nodes to join*
- *Persistent storage for transactions*
- *Merkle Patricia tree*
- *Transaction verification*

In the coming months, we plan to have the following features:

- *View change*
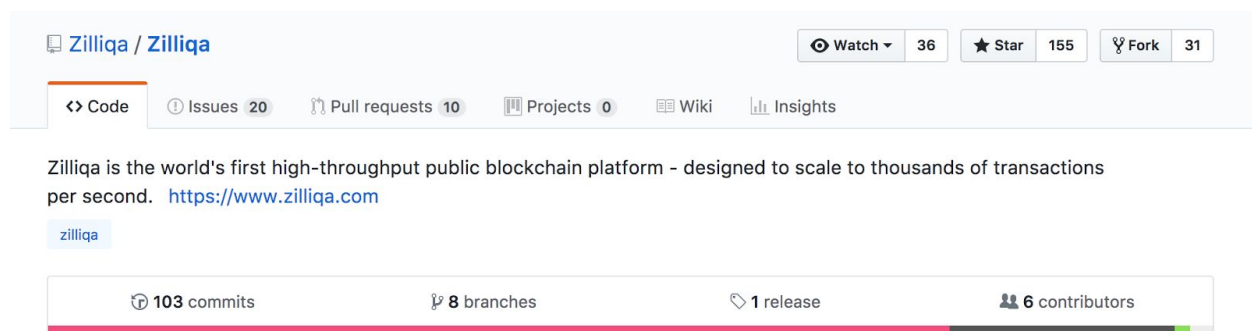- *Gossip protocol for network message broadcasting*

- *Incentive structure*
- *Smart contract design and implementation*
- *GPU support for PoW*
- *Zilliqa Wallet*
- *Further unit and integration tests*
- *Enhancement of existing features*
- *More operating system support*
- *And much more ...*

Version 0.1 was released on December 31, 2017 and the last commit was two days ago on the master branch.

The code is primarily written in C++ and C and is fairly well written, on the next page is a code sample from ConsensusCommon.cpp

```cpp
Signature ConsensusCommon::SignMessage(const vector<unsigned char> & msg, unsigned int offset, unsigned int size)
{
    LOG_MARKER();

    Signature signature;
    bool result = Schnorr::GetInstance().Sign(msg, offset, size, m_myPrivKey, m_pubKeys.at(m_myID), signature);
    if (result == false)
    {
        return Signature();
    }
    return signature;
}

bool ConsensusCommon::VerifyMessage(const vector<unsigned char> & msg, unsigned int offset, unsigned int size, const Signature
{
    LOG_MARKER();
    bool result = Schnorr::GetInstance().Verify(msg, offset, size, toverify, m_pubKeys.at(peer_id));

    if (result == false)
    {
        LOG_MESSAGE("Peer id: " << peer_id << " pubkey: 0x" << DataConversion::SerializableToHexStr(m_pubKeys.at(peer_id)));
        LOG_MESSAGE("pubkeys size: " << m_pubKeys.size());
    }
    return result;
}
```

The use of C++ classes to organize units of code make hte code extremely readable.

Their ERC20 smart contract token repository has also been audited and cleared for general use you can view the audits in the source code under the audit-reports directory.

Roadmap taken from their Reddit

Zilliqa roadmap self.zilliqa
14
Submitted 5 months ago by xinshudong · ZIL Core

Here is a tentative roadmap for about 1 year.
Jun 01, 2017: Project Zilliqa started
Aug 10, 2017: Whitepaper released
Sept 01, 2017: Experimental result release of internal testnet v0.1 (crypto, PoW, data layer, network sharding, consensus)
Oct 01, 2017: Experimental result release of internal testnet v0.5 (+ tx sharding & processing, storage, incentives, new nodes joining)
Nov 15, 2017: Releasing design documentation on smart contracts, compiler, and app framework; Experimental result release of internal testnet v1.0 (resilience & recover, wallet, optimizations)
Dec, 2017: Releasing public testnet v1.0 and source code (public miners can join and test, feedback & bug fixes)
Feb, 2018: Releasing public testnet v1.5 (with basic smart contract support)
Mar, 2018: Releasing public testnet v2.0 (with computational sharding)
Q2, 2018: Launching Zilliqa public mainnet
Q3, 2018: Releasing dApps

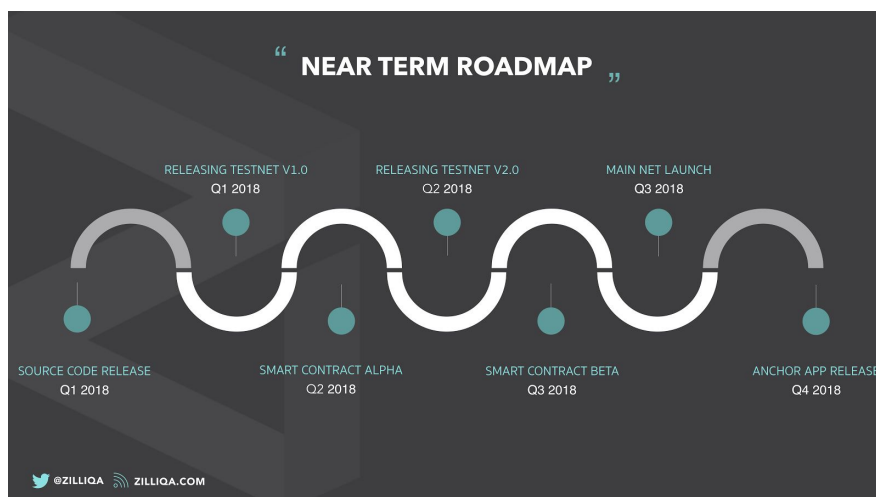Although the roadmap isn't as descriptive as we'd like it to be - we're pleased that it's technical.

Roadmap graphic taken from their Reddit page

Social Media
Telegram - 16,053 members
Twitter - 16.5K followers
Reddit - 3,067 readers

Markets

Zilliqa Markets

USD ▾

#	Source	Pair	Volume (24h)	Price	Volume (%)	Updated
1	Huobi	ZIL/BTC	$5,649,600	$0.074344	48.00%	Recently
2	Huobi	ZIL/ETH	$5,283,440	$0.074094	44.89%	Recently
3	EtherDelta	0x05f4/ETH	$249,330	$0.077800	2.12%	Recently
4	Gate.io	ZIL/USDT	$248,372	$0.074895	2.11%	Recently
5	Gate.io	ZIL/ETH	$228,111	$0.075421	1.94%	Recently
6	IDEX	ZIL/ETH	$109,914	$0.071603	0.93%	Recently

Conclusion

We rate Zilliqa as **fundamentally sound** for the long term - as long as they keep up with development of their blockchain that is being actively developed and meet their roadmap deadlines they should be in good shape. The team is excellent, the whitepaper is very technical and solid.